Transportation
Security
Administration

TSA Registered Traveler

Security, Privacy and Compliance Standards for Sponsoring Entities and Service Providers

Summary of Changes for RT Standards Version 2.1

November 27, 2006

Section/Paragraph	Change
1.2 Definitions	Added RTIC Technical Interoperability Specification Version 1.0: *"This document was developed by the Registered Traveler Interoperability Consortium (RTIC) to help foster a fully-interoperable, vendor-neutral Registered Traveler (RT) program within the United States."*
2.2/Para.1 Sentence 3	Change the wording to the following: *"One System Security Plan (SSP) shall be prepared for each system that forms the SP's RT IT program for each supported airport."*
3/Table 3-1	Credentialing Removed the following wording: *"-Display an SP return address."*
3/Table 3-1 Enrollment/Verification 3.4.3	Changed the wording to the following: *"-The SE/SP may not refuse service to an RT Participant regardless of the SE/SP with whom that person enrolled, as long as the SP has been certified as interoperable."*
3.3.4/#4	Added : *4. A Military ID Card issued by the Department of Defense provided it contains a photograph, information such as name, date of birth and security features capable of being verified through authentication technology, and has not declared invalid for identification purposes by the federal government AND any one of the following:* • *Certificate of Citizenship (Form N-560 or N-561)* • *Certificate of Naturalization (Form N-550 or N-570)* • *Valid U.S.-issued Permanent Resident Card or Alien Registration Receipt Card with photograph* • *Original or certified copy of U.S. birth certificate* • *Certificate of Birth Abroad issued by the Department of State (Form FS-545 or Form DS-1350)*
3.3.7/Para. 3	Changed the wording to the following: *"The SE/SP may develop a graphical user interface (GUI)-based enrollment application to collect and store the volunteered data."*

3.3.8	Added Section 3.3.8 <u>Update of Participant Biographic Data :</u> It Reads: *The RT participant may change or update biographic data. Changes could be due to relocation or marriage, affecting contact information or name change. Updates to participant data may also occur in order to correct errors.* *Some changes in participant biographic data may require re-assessment of the participant's Security Threat Assessment status. The SE/SP shall attempt to collect participant biographic data updates within 30 days of any change to participant biographic data, but in all cases shall collect updated biographic data from participants on an annual basis.* *The SE/SP shall re-verify participant identity documents and re-capture digital images of participant identity documents as specified in section 3.3.4, whenever a participant reports changes or updates to any of the following biographic information to the SE/SP:* • *Name;* • *Gender;* • *Date Of Birth;* • *Citizenship status;* • *Place Of Birth;* • *Social Security Number;* • *Alien Registration Number;* • *Driver's license number and State;* • *Passport Type;* • *Passport Number*. **Note:** Adding this section subsequently affected the following section numbers: *"Biometric Data Collection", "Separation of Biographic and Biometric Information", "Credential", & "Notification of Eligibility"*
3.3.11/Para. 3 & 4	Changed the wording to the following: *"A user's private information stored in his or her card shall be stored in a protected state while at rest (the card is disengaged from a valid verification station). A secret key (KC) shall be used to restrict access to the private authentication data using 3DES. The RT card will not reveal the private information until the authentication protocol succeeds with the verification station and the HSM that holds the master secret.* *In the event that the KC is compromised (for example, the RT card is lost or stolen), then a new card shall be provided to the RT participant. This card will utilize a new KC that is used to protect the private information on the card while it is disengaged from the verification station."*
3.3.12/ Para. 2	Changed the wording to the following: *"The SP shall develop a process allowing for the daily processing of all newly updated RT Participant status files from CIMS. SPs shall notify CIMS when a card should be deactivated (when lost, stolen, malfunctioning, etc.) within 24 hours."*
3.4.1/Para. 5	Changed the wording to the following: *"The SE/SP shall ensure that the traveler's name on the RT card or government issued photo identification matches the name on the boarding pass."*

4.2.1	Removed the national security background investigation requirement in the last sentence:*"In addition, IPA personnel involved in performing the attestation must have a national security background investigation; given the sensitive nature of the controls SPs will have in place (or not in place) to protect PII."*
Appendix B	Formatting and cosmetic changes.
Appendix C - AC-18 WIRELESS ACCESS RESTRICTIONS	Removed *"Examine organizational records or documents to determine if the access control policy and procedures are consistent with NIST Special Publication 800-48 and address usage, implementation, monitoring, and authorization of wireless technologies."*
Appendix C - CA-3 INFORMATION SYSTEM CONNECTIONS	Removed *"Examine information system connection agreements to determine if theagreements are consistent with NIST Special Publication 800-47."*
Appendix C - CA-3 INFORMATION SYSTEM CONNECTIONS	Removed *"Examine organizational records or documents to determine if the organization employs a security certification process in accordance with NIST Special Publications 800-37 and 800-53A."*
Appendix C - CA-6 SECURITY ACCREDITATION	Removed *"Examine organizational records or documents to determine if the security accreditation process employed by the organization is consistent with NIST Special Publications 800-37."*
Appendix C - CA-7 CONTINUOUS MONITORING	Removed *"Examine organizational records or documents to determine if the organization employs a security control monitoring process consistent with NIST Special Publications 800-37 and 800-53A."*
Appendix C - CP-2 CONTINGENCY PLAN	Removed *"Examine the contingency plan for the information system to determine if the plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities for restoring the information system consistent with NIST Special Publication 800-34."*
Appendix C - MP-6 MEDIA SANITIZATION AND DISPOSAL	Removed *"Examine organizational records or documents to determine if the organization sanitizes information system media, both paper and digital, using approved equipment, techniques, and procedures prior to disposal or release for reuse consistent with NIST Special Publication 800-88."*
Appendix C - PL-2 SYSTEM SECURITY PLAN	Removed *"Examine the security plan to determine if the plan is consistent with NIST Special Publication 800-18 and addresses security roles, responsibilities, assigned individuals with contact information, and activities for planning security of the information system. Interview selected organizational personnel with security planning and plan implementation*
Appendix C - PL-4 RULES OF BEHAVIOR	Removed *"Examine the rules of behavior to determine if the content is consistent with NIST Special Publication 800-18."*
Appendix C - PS-7 THIRD-PARTY PERSONNEL SECURITY	Removed *"Examine organizational records or documents to determine if the organization explicitly includes personnel security requirements in acquisition-related documents in accordance with NIST Special Publication 800-35."*
Appendix C - RA-2 SECURITY CATEGORIZATION	Removed *"Examine the system security plan to determine if the security categorization of the information system: (i) exists; (ii) is consistent with FIPS 199; (iii) includes supporting rationale consistent with NIST Special Publication 800-60; and (iv) is reviewed and approved by designated senior-level officials within the organization."*

Appendix C - RA-3 RISK ASSESSMENT	Removed *"Examine the risk assessment for the information system to determine if the assessment is consistent with NIST Special Publications 800-30 and 800- 95."*
Appendix C - RA-5 VULNERABILITY SCANNING	Removed *" Examine the latest vulnerability scanning results to determine if patch and vulnerability management is handled in accordance with NIST Special Publication 800-40 (Version 2)."*
Appendix C - SA-8 SECURITY DESIGN PRINCIPLES	Removed *"Examine organizational records or documents to determine if the organization considers security design principles in the development and implementation of the information system consistent with NIST Special Publication 800-27."*
Appendix F	Added the following references: Department of Homeland Security Department of Homeland Security. DHS 4300.1. *Information Technology Systems Security* Transportation Security Administration Transportation Security Administration. (2006). *TSA Information Security Handbook 1400.3-Information Security Policy*